8

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/446,525	12/27/1999	MASAYUKI KANDA	162/540	2460

7590 12/09/2003

POLLOCK VANDE SANDE & PRIDDY
PO BOX 19088
WASHINGTON, DC 20036-3425

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2131	7

DATE MAILED: 12/09/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

8

Office Action Summary	Application No.	Applicant(s)	
	09/446,525	KANDA ET AL.	
	Examiner	Art Unit	
	Michael R Vaughan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 November 2003*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *14-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *14-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 December 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

Detailed Action

The communication filed on 11/13/03 amended the title and claims. Claims 14-49 are pending.

Response to Argument

Applicant's arguments filed November 13, 2003 have been fully considered but they are not persuasive.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., *the entire bits of a block data supplied to each nonlinear function part, such as 304 in Fig. 3, is subjected to nonlinear processing by first and second nonlinear transformation parts such as 343-346 and 348-351 in Fig. 4, the total number of cascade processing stages for nonlinear transformation parts in the cascade-connected round processing parts* 38_0*-*38_{n-1} *is two times the number of round processing parts, and the cryptographic process according to the present invention can be easily adapted to encrypt input data in an increased length without lowering the processing speed*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Regarding Claim 14, applicants argue:

The Matsui reference describes a type or encryption system known as MISTY 1 and MISTY 2. According to the reference, a 64-bit data block is divided into a left 32-bit data block and a right 32-bit data block. The left 32-bit data block is transformed in each of the plurality of round processing stages to be transformed by an FO-function, and that result is XORed with the right 32-bit data block. The XORed output and the right 32-bit data block are switched with each other. The 32-bit block data from both the left and right are then input to a subsequent round processing stage. The FO function in each round processing stage is constructed as a double nestled three round process, shown in Fig. 4, and the block size of data supplied to each of the s-functions in the lowest level is only 9-bits which allows the use of nonlinear transformers (I.E., s-functions) of a smaller size while achieving a higher robustness.

According to Fig. 4, since each FO-function is a k-nestled 3-round processing stage, the total number of s-functions in series becomes 3k times as many as the case in which each FO-function is a single s-function. Encryption processing speed is roughly inversely proportional to the number of s-functions in series, which means that the MISTY1 and MISTY 2 encryption schemes have a lower encryption processing speed.

This is to be distinguished from the present invention. According to the present invention, the entire bits of a block data supplied to each nonlinear function part, such as 304 in Fig. 3, is subjected to nonlinear processing by first and second nonlinear transformation parts such as 343-346 and 348-351 in Fig. 4, and as set forth in rejected claim 14. Accordingly, the total number of cascade processing stages for nonlinear

transformation parts in the cascade-connected round processing parts 38_0-38_{n-1} is two times the number of round processing parts and therefore encryption processing speed is much faster than in the MISTY devices. The data input to each nonlinear function part such as 304 is split by a splitting part such as 342 into plural bit springs and individually processed by a plurality of first nonlinear transformation parts such as 343-346. The cryptographic process according to the present invention can be easily adapted to encrypt input data in an increased length without lowering the processing speed. This feature cannot be obtained from the MISTY1 or 2 systems.

It is clear, that the present invention as defined by claim 14 is not suggested by the combination of DES and Matsui. As noted above, numerous features of the applicants claims, such as splitting data using a splitting part into plural bit strings, and then processing the plural bit strings using nonlinear transformation parts, remains undisclosed or suggested when the references are combined as suggested in the Office Action.

The examiner maintains that all of the limitations of claim 14 are taught by DES in view of Matsui.

DES teaches:

An initial splitting part (FIG. 1);

A key storage part (inherent in view of FIG. 1);

A plurality of cascade-connected round processing parts which are supplied with said two pieces of block data and sequentially process them using said extended key (FIG. 1);

A final combining part which combines two pieces of block data output from the last round (FIG. 1);

Wherein each of said plurality of round processing part comprises:

A non-linear function part (FIG. 1);

A linear operation part (FIG. 1);

A swapping part which swaps the output data from said linear operation part and input block data to said nonlinear function part and provides the two pieces of swapped data as two pieces of input block data to said round processing part of the next round (FIG. 1); and

Wherein said nonlinear function part comprises:

A key-dependent linear transformation part (FIG. 2);

A splitting part, which splits the transformed data from said key-dependent linear transformation part to a plurality of bit strings (FIG. 2);

A plurality of first nonlinear transformation parts (FIG. 1);

A first linear transformation part which linearly transforms said transformed data from said plurality of first nonlinear transformation parts in association with each other and output a plurality of pieces of uniformed data to a plurality of routes (FIG. 2);

A combining part, which combines data from, said plurality of routes into output data of said nonlinear function part (FIG. 2).

From the teachings of DES, all of the limitations of claim 14 are taught with the exception of a second nonlinear transformation part provided in at least one of said

plurality of routes, for nonlinearly transforming said transformation parts, and for outputting the transformed data as data of that route.

Matsui's MISTY algorithms are block ciphers that operate very much like DES. Matsui designed his algorithm to protect a block cipher from differential and linear cryptanalysis (pg. 1). He teaches that his recursively nonlinear functions are strong against such attacks (pg. 1). He also teaches that MISTY should be fast enough to run in both software and hardware (pg. 1). Matsui teaches that his primary design policy was to make MISTY strong against differential and linear cryptanalysis (pg. 1). To accomplish his goals he implemented a second nonlinear transformation part provided in at least one of said plurality of routes, for nonlinearly transforming said transformation parts, and for outputting the transformed data as data of that route (FIG. 4). Now referring to FIG. 4, Matsui teaches in FO Level2 that the bits are broken up (split up) into two parts, which are then fed into nonlinear transformation parts in a series of rounds. It is clear from FIG. 4 that data is split using a splitting part into plural bit strings, and then processing the plural bit strings using nonlinear transformation parts. The teachings of DES in view of Matsui meet all of the limitation as disclosed in applicant's claim 14.

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Matsui into an algorithm such as DES. Matsui teaches that the strength is greater because of the added nonlinear parts and the speed is suitable for even high-speed ATM network applications (pgs. 1 and section 4.1).

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

In response to the rejection of claims 28, 29, 32, 33, 36, 37, 42, 43, 46, and 47, the applicant argues that *the allegation that claims 28, 29, 32, 33, 36, 37, 42, 43, 46, and 47 are obvious in view of Matsui and DES appear to be the result of an impermissible use of hindsight. While the teachings of Kwan (The Design of the ICE: Encryption Algorithm) may disclose data being broken into four parts, is not considered that Kwan when combined with DES and Matsui would yield or disclose the specific subject matter of claims 28 which require four specific routes.*

The examiner maintains that claims 28, 29, 32, 33, 36, 37, 42, 43, 46, and 47 would have been obvious over DES in view of Matsui in further view of ICE. DES teaches the use of S-boxes (FIG 2.) Matsui teaches running the data through multiple S-boxes within each round of transformation. ICE teaches the use of four 8-bit output S-boxes (see Section 4). DES teaches 8 S-boxes whose outputs are combined to yield a 32-bit output. The output of ICE is also 32 bits. ICE chooses to use S-boxes, which

use Galois Field exponentiation and are proven resistant to differential cryptanalysis (see Section 4). Substituting the S-boxes of ICE within the system of DES would have been obvious to one of ordinary skill in the art of the time of the invention because increasing an encryption algorithm's resistance to cryptanalysis is highly desirable. In view of this, the motivation as taught by ICE was used to show why it would have been obvious to one of ordinary skill in the art to employ the teachings of ICE with in the system of DES and Matsui.

In response to the rejection of claims 30, 34, 38, 44, and 48, the applicant argues that the *allegation that claims 30, 34, 38, 44, and 48 are obvious in light of the combined teachings of DES and Matsui are similarly believed to be the result of hindsight. The elements of these claims requiring first through fourth routes, followed by a nonlinear transformation appears unsuggested in any of the references, or any combination of the cited references.*

The examiner maintains that claims 30, 34, 38, 44, and 48 would have been obvious over DES in view of Matsui in further view of ICE. The use of four 8-bit output S-boxes along four routes within recursive rounds within a DES algorithm was shown obvious as recited by examiner above. The examiner maintains that it would have been obvious to one of ordinary skill in the art at the time of the invention to eliminate some of the recursive S-box transformations in order to comply with a system's capabilities. If performing all 4 S-box transformations in each round took to much time, some could have been omitted to save valuable calculation time. Any one of the four S-boxes could

have been omitted within the recursive rounds, including the second and third S-boxes as disclosed in claims 30, 34, 38, 44, and 48.

The examiner also recites legal precedent of *In re Karlson*, 311 F.2d 581, 583, 136 USPQ 184, 186 (CCPA 1963) and *In re Kuhle*, 526 F.2d 553, 188 USPQ 7 (CCPA 1975) whereby the Court ruled that eliminating element and its functions was deemed obvious.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 14-27, 40, and are rejected under 35 U.S.C. 103(a) as being unpatentable over DES (Data Encryption Standard, National Bureau of Standards (U.S.), in view of Matsui (New Block Encryption Algorithm MISTY).

As per claim 14, DES teaches:

initial splitting of data (FIG. 1);

Key storage (inherent) (FIG. 1);

Plurality of rounds cascaded together (FIG. 1);

Final combining part (inverse initial permutation) (FIG. 1);

Non-linear function (f) (FIG. 1);

Linear operation part (XOR) (FIG. 1);

Swapping part (FIG. 1);

Key-dependent linear transformation part within the nonlinear function (FIG. 2);

Splitting part (FIG. 2);

Plurality of first nonlinear transformation parts (FIG. 2)

First linear transformation part (FIG. 2);

Combining part (p) (FIG. 2).

DES is silent in disclosing a second nonlinear transformation part. Mitsui teaches a plurality of nonlinear parts to operate on data. Mitsui teaches that within each round of ciphering, the data passes through S-boxes (nonlinear transformation parts) more than once (FIG. 4). Linear transformations occur between S-boxes. Mitsui teaches that computation is faster when the size of the data is small (page 1). It is notoriously well known in the art that the strength of DES like algorithms rely on the nonlinear transformations. Therefore, it is obvious that there need to be many nonlinear transformations. MISTY, as taught by Mitsui has increased the number of nonlinear transformation by subjecting the data to several sets of S-boxes in each round. In view of this, it would have been obvious to one of ordinary skill in the art to use two sets of nonlinear transformation within each round of a DES like algorithm.

As per claim 15, DES teaches the use of keys in a linear transformation prior to going into the S-boxes on a plurality of routes (FIG 2).

As per claims 16, 17, 19, and 20, DES teaches that a linear transformation using the secret key is performed in each round (FIG 2). DES performs this function at the start of the nonlinear function. Performing the exact same linear function again at the end of the nonlinear function does not constitute a novel difference. DES teaches the linear function and using it twice in the same round does not part from the scope of the prior art.

As per claims 18 and 21, DES teaches linearly combining the key and the data (FIG 2). It is notoriously well known in the art that XOR'ing is function to linearly combine bits. Therefore, it is inherent that the data can be XOR'ed with the key, bit by bit.

As per claims 22, 23, 24, 25, 26, 27 and 40, and 41, the scope of DES teaches the use of performing a linear transformation to the input data and a secret key. Using an additional initial and final linear transformation functions does not constitute a novel difference.

Claim 28, 29, 30, 32, 33, 34, 36, 37, 38, 42, 43, 44, 46, 47, and 48 rejected under 35 U.S.C. 103(a) as being unpatentable over DES and Mitsui as applied to claims 14, 22, 23, 24, 25, 26, and 40 above, and further in view of Kwan (The Design of the ICE Encryption Algorithm).

As per claims 28, 29, 32, 33, 36, 37, 42, 43, 46, and 47, the combined teachings of DES and Matsui are silent in disclosing that there are explicitly four routes. The combination of Matsui's recursive S-box structure into the DES algorithm makes having multiple S-boxes functions obvious within each round. The teaching of Kwan discloses,

in his ICE algorithm, that he breaks the data into four parts, which traverse down four paths (FIG. 2). Each path leads to a nonlinear S-box. Kwan chooses to break down the data into four pieces contrary to Matsui's two pieces. Both authors break down the chunks whereby the calculations can be performed efficiently within the resources of the device. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to have four routes leading to the nonlinear transformation devices.

As per claims 30, 34, 38, 44, and 48, the combined teachings of DES and Matsui are silent in disclosing that in the first and fourth routes lead to a second nonlinear transformation. The examiner sites the same rationale for motivation as recited in the rejection of claims 28, 29, 32, 33, 36, 37, 42, 43, 46, and 47. The motivation behind having more than one nonlinear transformation in each round is to increase the strength of the algorithm in a fewer number of rounds. These additional computations require more time and resources. It is well known in the art that DES like algorithms base their strength in the nonlinear transformations. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to increase the number of nonlinear transformation by routing some of the data chunks through a second nonlinear transformation. Of the four routes, any number of them could be sent to the second nonlinear transformation. The motivation is to balance the strength of the algorithm within the confines of the resources.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

MV
Michael R Vaughan
Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100